Daily Open Source Infrastructure Report
28 September 2015

Top Stories

- Hyundai Motor Co., issued a recall for 470,000 model years 2011 – 2012 Sonata 2-liter and 2.4-liter sedans due to an issue with metal debris in the car's crankshaft which could lead to an engine stall. – *Associated Press* (See item **4**)
- Four international students from North Seattle College were killed and 51 others were injured September 24 after a charter bus filled with 45 students collided with a "duck tour" vehicle on Seattle's Aurora Bridge. – *NBC News* (See item **10**)
- Authorities reported September 24 that a combination of 12 inmates, prison employees, parolees, and civilians were allegedly found to be a part of a drug and identity theft ring taking place in Georgia prisons. – *WXIA 11 Atlanta* (See item **20**)
- U.S. regulators reported September 24 that Hamilton Relay, InnoCaption, and Sprint Corp., reached a $1.4 million settlement resolving allegations over the companies' 9-1-1 handling for hard-of-hearing callers. – *U.S. Federal Communications Commission* (See item **27**)

Fast Jump Menu

Energy Sector

1. *September 25, Muskegon Chronicle* – (Michigan) **Grand Haven utility to dismantle two 400,000-gallon oil tanks.** The Grand Haven Board of Light & Power will remove two, 400,000 gallon oil above ground oil tanks near Mulligan's Hollow in Michigan beginning September 28 due to the storage tanks no longer being in use. Environmental assessments will be conducted following the tanks' removal and the space will be repurposed by the City of Grand Haven.
   Source: http://www.mlive.com/news/muskegon/index.ssf/2015/09/grand_haven_utility_to_dismant.html

2. *September 24, Duluth News Tribune* – (Minnesota) **700 barrels of dyed water spilled in Enbridge test failure.** Enbridge Energy reported that an estimated 29,400 gallons of test water was released following equipment failure while workers were preparing for hydrostatic dye testing on a segment of Pipeline 2B near Floodwood September 23. Crews reported to the site, contained the leak, and worked to cleanup and assess any environmental effects.
   Source: http://www.duluthnewstribune.com/news/3846632-700-barrels-dyed-water-spilled-enbridge-test-failure

For another story, see item **22**

Chemical Industry Sector

3. *September 24, Associated Press* – (Colorado) **Army halts chemical weapons destruction in Colorado.** Official reported September 24 that the U.S. Army temporarily stopped all destruction of chemical weapons at the Pueblo Chemical Depot in Colorado after crews discovered a dent in a chamber door used to explode and neutralize shells containing mustard agent August 7. Officials believe that the dent was caused by a metal fragment that was caught in the door when it closed and locked under pressure, and operations were estimated to resume October 5.
   Source: http://www.msn.com/en-us/news/us/army-halts-chemical-weapons-destruction-in-colorado/ar-AAeKedE

For another story, see item **22**

Nuclear Reactors, Materials, and Waste Sector

See item **22**

Critical Manufacturing Sector

4. *September 25, Associated Press* – (National) **Hyundai recalls 470,000 Sonatas to fix critical engine problem.** Hyundai Motor Co., issued a recall for 470,000 model years 2011 – 2012 Sonata 2-liter and 2.4-liter sedans due to the possible presence of metal debris in the car's crankshaft, which could restrict oil flow and lead to an engine stall.

Owners will be notified November 2.
Source: http://www.cnbc.com/2015/09/25/hyundai-recalls-470000-sonatas-to-fix-critical-engine-problem.html

For another story, see item **22**

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *September 24, U.S. Securities and Exchange Commission* – (International) **SEC charges six in stock fraud scheme.** The U.S. Securities and Exchange Commission charged 6 suspects for an investment scheme in which the suspects allegedly conspired to secretly issue $72 million Gerova shares to a family friend in Kosovo through a friend's brokerage accounts, while bribing an investment adviser to stabilize Gerova shares in 2010. The suspects reportedly received at least $16 million in illicit profits through the scheme, and face criminal charges under a separate parallel action.
Source: http://www.sec.gov/litigation/litreleases/2015/lr23360.htm

6. *September 24, Reuters* – (New Jersey) **New Jersey's Hudson City Bank to pay some $33 mln in redlining case.** Hudson City Bancorp agreed September 24 pay $33 million in loan subsidies, community programs and outreach, and penalties to settle U.S. Department of Justice and Consumer Financial Protection Bureau allegations that the company discriminated against prospective black and Hispanic home buyers by attempting to avoid locating branches and marketing mortgages in neighborhoods with a majority of black and Hispanic residents.
Source: http://www.reuters.com/article/2015/09/24/hudson-city-bcp-discrimination-idUSL1N11U1T320150924

7. *September 24, Newark Patch* – (New Jersey) **N.J. bank fraud: Founder of defunct charter flight company pleads guilty.** The former chief financial officer and co-founder of Southern Sky Air & Tours pleaded guilty September 23 to conspiracy to commit wire and bank fraud through a scheme in which he used fake documents and inflated revenue figures to defraud a New Jersey bank and other financial institutions out of millions of dollars.
Source: http://patch.com/new-jersey/newarknj/nj-bank-fraud-founder-defunct-charter-flight-company-pleads-guilty

8. *September 24, InsideNoVa.com* – (National) **'Black Hat Bandit' pleads guilty to 9 bank robberies.** The suspect dubbed the "Black Hat Bandit" pleaded guilty September 24 in connection to 9 bank robberies throughout Virginia, Maryland, and Washington, D.C. earlier this year from January – March and resulted in more than $180,000 in losses to BB&T and Wells Fargo bank branches that he struck.
Source: http://www.insidenova.com/headlines/black-hat-bandit-pleads-guilty-to-bank-robberies/article_a417d4f4-62e0-11e5-b049-df27a854c2b7.html

9. *September 24, IDG News Service* – (International) **New malware infects ATMs, dispenses cash on command.** Security researchers from Proofpoint detected a new malware ATM malware program dubbed GreenDispenser that allows attackers to withdraw cash on demand by hooking into the eXtensions for Financial Services (XFS) middleware on Microsoft Windows-based ATMs. The malware was first spotted in Mexico, and researchers warned it will likely spread quickly to the U.S.
Source: http://www.computerworld.com/article/2985860/malware-vulnerabilities/new-malware-infects-atms-dispenses-cash-on-command.html#tk.rss_security

Transportation Systems Sector

10. *September 25, NBC News* – (Washington) **Four college students killed when duck boat and charter bus crash in Seattle.** The National Transportation Safety Board is investigating a September 24 incident where 4 international students from North Seattle College were killed and 51 people were injured after a charter bus filled with 45 students collided with a "duck tour" vehicle on the Aurora Bridge in Seattle.
Source: http://www.nbcnews.com/news/us-news/seattle-bus-collides-duck-tour-killing-2-officials-say-n433156

11. *September 24, KXAS 5 Fort Worth* – (Texas) **2 killed in fiery plane crash at Granbury Municipal Airport.** The Federal Aviation Administration and the U.S. National Transportation Safety Board are investigating a single-engine plane crash in Hood County that killed two people September 24. The plane went down shortly after take-off and burst into flames at Granbury Municipal Airport.
Source: http://www.nbcdfw.com/news/local/Plane-Crash-at-Granbury-Municipal-Airport-329337281.html

12. *September 24, Atlanta Journal-Constitution* – (Georgia) **Tarantula delays Delta Air Lines flight from Baltimore to Atlanta.** Delta Air Lines Flight 1525 from Baltimore to Atlanta was delayed for approximately 3 hours September 23 to search the aircraft after baggage handlers found a baboon tarantula out of its carrier. No injuries were reported.
Source: http://www.ajc.com/news/news/tarantula-delays-delta-air-lines-flight-from-balti/nnnLz/

13. *September 24, Victor Valley News* – (California) **Fatal motorcycle collision causes shut down of Highway 395.** North and Southbound lanes of Highway 395 in Adelanto were shut down for several hours September 24 while the Major Accident Investigation Team responded to a fatal accident that involved a motorcycle and a vehicle, and killed 1 person.
Source: http://www.vvng.com/fatal-motorcycle-collision-causes-shut-down-of-highway-395/

For another story, see item **22**

Food and Agriculture Sector

14. *September 25, U.S. Department of Agriculture* – (Georgia; Louisiana) **Sanderson Farms recalls poultry products due to possible foreign matter contamination.** Hazlehurst, Mississippi-based Sanderson Farms issued a recall for approximately 554,090 pounds of its poultry products September 24 after the company received complaints from a processing facility following the discovery of metal shavings in the products. The items were shipped to processing facilities in Georgia and Louisiana.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-124-2015-release

For another story, see item **22**

Water and Wastewater Systems Sector

15. *September 25, Long Beach Press-Telegram* – (California) **Long Beach partially reopens beaches after recent sewage spill.** Long Beach officials reopened coastal beaches east of Molino Avenue September 25 after testing showed bacterial levels are within safe range following a September 15 sewage spill in San Gabriel. The beaches west of Molino Avenue will remain closed until testing shows improvement in water quality.
Source: http://www.presstelegram.com/environment-and-nature/20150924/long-beach-partially-reopenes-beaches-after-recent-sewage-spill

16. *September 24, Austin American-Statesmen* – (Texas) **Water main break in Pflugerville causes half-million gallon leak.** The Windermere Utility Company turned off the water supply after a Pflugerville city contractor accidentally hit an 8-inch line, causing 560,000 gallons of chlorinated water to spill into Gilleland Creek September 23. The creek is closed to the public while officials investigate the scene.
Source: http://www.statesman.com/news/news/local/water-main-break-in-pflugerville-causes-half-milli/nnnJR/

17. *September 24, CBS News* – (Nevada) **Las Vegas uncaps Lake Mead's "third straw" for water supply.** The Southern Nevada Water Authority reported that the 6-year "Third Straw" project to draw drinking water from Las Vegas from Lake Mead was completed September 23 after an intake was unplugged. The project was designed to maintain water flow to Las Vegas even if the drought-stricken lake drops to its lowest levels.
Source: http://www.cbsnews.com/news/las-vegas-uncaps-lake-meads-third-straw-for-water-supply/

For another story, see item **22**

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

18. *September 25, KTMF 23 Missoula* – (Montana) **Classes canceled at Big Sky High School.** A power issue prompted school administrators to cancel classes at Big Sky High School in Missoula September 25. Crews from NW Energy were working to repair the problem.
Source: http://www.abcfoxmontana.com/story/30116130/classes-canceled-at-big-sky-high-school

19. *September 24, WNEP 16 Scranton* – (Pennsylvania) **Marywood University campus closed by bomb threats.** Students and staff were evacuated and classes were cancelled at Marywood University in Scranton September 24 following two phoned bomb threats. Police and fire officials reported to the campus to investigate the threats.
Source: http://wnep.com/2015/09/24/marywood-university-campus-closed-till-further-notice/

For another story, see item **3**

Emergency Services Sector

20. *September 24, WXIA 11 Atlanta* – (Georgia) **12 indicted in prison cell phone bust.** Authorities announced September 24 that a combination of 12 inmates, prison employees, parolees, and civilians were allegedly part of a drug and identity theft ring that took place in Georgia prisons. The scheme reportedly involved smuggling prescription pain medication, illegal drugs, alcohol, tobacco, and cell phones into the prisons where the inmates would use the phones to steal identities from victims in Cobb and Gwinnett counties.
Source: http://www.11alive.com/story/news/crime/2015/09/24/12-indicted-prison-cell-phone-bust/72768876/

21. *September 24, KCRA 3 Sacramento* – (California) **3 officers injured in separate attacks at New Folsom prison.** Sacramento County officials are investigating after 3 correctional officers were injured September 24 in 2 separate incidents at California State Prison-Sacramento. Guards attempted to stop a stabbing between inmates and were attacked by several other inmates before being subdued with pepper spray and a warning shot, while a third guard was injured after being struck in the back of the head by an inmate.
Source: http://www.kcra.com/news/local-news/news-sacramento/3-officers-injured-in-separate-attacks-at-new-folsom-prison/35470110

For another story, see item **27**

Information Technology Sector

22. *September 25, Securityweek* – (International) **Vulnerabilities found in several SCADA products.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published advisories identifying vulnerabilities in supervisory control and

data acquisition (SCADA) products, including a privilege escalation bug in Resource Data Management's Data Manager that could allow an attacker to change the passwords of users, a cross-site request forgery (CSRF) that an attacker could use to perform actions on behalf of authenticated users, and other vulnerabilities in IBC Solar and EasyIO products.
Source: http://www.securityweek.com/vulnerabilities-found-several-scada-products

23. *September 25, Help Net Security* – (International) **Cisco releases tool for detecting malicious router implants.** Cisco Systems released a Python script called the SYNful Knock Scanner which scans networks for routers compromised by malicious SYNful Knock implants and provides next steps to users with affected routers.
Source: http://www.net-security.org/malware_news.php?id=3114

24. *September 25, The Register* – (International) **XcodeGhost-infected apps open gates to malware hijacking.** Security researchers from Palo Alto Networks reported that the DES ECB mode-encrypted communication streams between XcodeGhost-infected applications and the attacker's command-and-control (C&C) servers lack proper encryption, leaving them vulnerable to man-in-the-middle (MitM) attacks that could expose affected users to additional malware.
Source: http://www.theregister.co.uk/2015/09/25/xcodeghost_mitm_palo_alto/

25. *September 25, Softpedia* – (International) **Kovter malware now lives solely in the Windows registry.** Security researchers from Symantec discovered a new version of the Kovter trojan that reportedly mimics the Poweliks malware's survival methods, including the ability to hide its code in the Microsoft Windows registry, ensuring persistence and serving as an entry point for other malware. The Kovter trojan focuses primarily on click-fraud, and 56 percent of all infections have targeted U.S. users.
Source: http://news.softpedia.com/news/kovter-malware-now-lives-solely-in-your-computer-s-registry-492722.shtml

26. *September 24, Threatpost* – (International) **Cisco patches denial-of-service, bypass vulnerabilities in IOS.** Cisco released updates for its IOS router and switch software addressing three denial-of-service (DoS) vulnerabilities and one authentication bypass flaw affecting RSA-based user authentication in which an attacker knowing a legitimate username and the user's public key could log in with their privileges.
Source: https://threatpost.com/cisco-patches-denial-of-service-bypass-vulnerabilities-in-ios/114792/

For another story, see item **9**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

27. *September 24, U.S. Federal Communications Commission* – (National) **Companies fined $1.4 million for failing to accept 911.** The U.S. Federal Communications Commission's (FCC) Enforcement Bureau reported September 24 that Hamilton Relay, InnoCaption, and Sprint Corp., reached a settlement totaling $1.4 million to resolve allegations of the companies' inability to handle 9-1-1 calls through applications used by callers who are hard of hearing over periods varying from 5 weeks to approximately 10 months.
Source: https://www.fcc.gov/document/cos-fined-14m-failing-accept-911-calls-hearing-impaired-0

Commercial Facilities Sector

28. *September 24, St. Petersburg Bay News 9* – (Florida) **Cousins charged in 35 commercial burglaries throughout Florida.** Officials reported September 24 that two men were arrested and charged in connection to a stealing nearly $80,000 in cash through a series of commercial burglaries targeting approximately 35 pizza carryout/delivery restaurants throughout Florida over a 9-month period.
Source: http://www.baynews9.com/content/news/baynews9/news/article.html/content/news/articles/bn9/2015/9/24/cousins_charged_in_3.html

Dams Sector

See item **22**

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer